34.	An "Oil and Vinegar" signature generating apparatus according to claim 32 and wherein a number v of "vinegar" variables is selected to satisfy the inequalities $v < n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic $p=2$ of a field K in an "Oil and Vinegar" scheme of degree 2, where n is a number of "oil" variables, K is a finite field from which the n "oil" variables and the v "vinegar" variables are selected, and q is the number of elements of K.

35.	A digital signature comprising:

a signature $e_1,...,e_{n+v}$ generated by processing a set S1 of k polynomial functions provided as a public-key and a message to be signed, where the set S1 includes functions $P_1(x_1,...,x_{n+v}, y_1,...y_k),...,P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k (x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,...,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v}, y_1,...y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$, so that a hash function applied on the message to produce a series of k values $b_1,...,b_k$ that are substituted for the variables $y_1,...,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),..., P''_k(a_1,...,a_{n+v})$ and v values $a'_{n+1},...,a'_{n+v}$ that are selected for the v "vinegar" variables $a_{n+1},...,a_{n+v}$, enable to solve a set of equations $P''_1(a_1,...,a_n, a'_{n+1},...,a'_{n+v})=0,...,P''_k(a_1,...,a_n, a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$, and application of the secret key operation transforms $a'_1,...,a'_{n+v}$, into the digital signature $e_1,...,e_{n+v}$.

36.	A digital signature produced by the method of claim 1.--

REMARKS

Applicant intends this Preliminary Amendment to place the application in better condition for examination. Favorable consideration and allowance of the application are respectfully requested.

Claims 2 - 10 and 15 - 17 have been amended for clarification.

NDS-4600

New claims 18 - 36 have been added.

Apparatus claims 18 - 34 correspond to method claims 1 - 17. Claim 35 recites a digital signature. Claim 36 recites a product of the method of claim 1.

Claim 18 is supported, inter alia, by the specification from the second paragraph on page 8 through the third full paragraph on page 10, and by Fig. 1.

Claim 19 is supported, inter alia, by the fourth paragraph on page 8 of the specification.

Claim 20 is supported, inter alia, by the paragraph bridging pages 10 and 11 of the specification.

Claims 21 and 22 are supported, inter alia, by the first full paragraph on page 11 of the specification.

Claims 23 and 24 are supported, inter alia, by the third full paragraph on page 11 of the specification.

Claim 25 is supported, inter alia, by the fourth full paragraph on page 11 of the specification.

Claims 26 and 27 are supported, inter alia, by the specification from the second full paragraph on page 12 through the first full paragraph on page 13.

Claim 28 is supported, inter alia, by lines 2 - 4 on page 10 of the specification.

Claims 29 and 30 are supported, inter alia, by the second full paragraph on page 13 of the specification.

Claim 31 is supported, inter alia, by the fourth paragraph on page 8 of the specification, and by the paragraph bridging pages 10 and 11 of the specification.

Claim 32 is supported, inter alia, by the first full paragraph on page 12 of the specification.

Claims 33 and 34 are supported, inter alia, by the specification similarly to claims 26 and 27.

Claim 35 is supported, inter alia, by the specification similarly to claim 18.

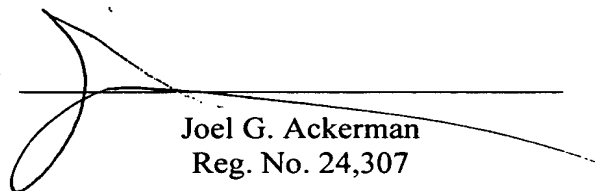Claim 36 is supported, inter alia, by originally filed claim 1.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is now in position for allowance. Favorable consideration and allowance of the application are respectfully requested.

NDS-4600

Respectfully submitted,

LIMBACH & LIMBACH L.L.P.

Dated: _12/19(2000)_   By: _____

Joel G. Ackerman
Reg. No. 24,307

Attorneys for Applicant(s)

Attorney Docket No. NDS-4600